2020-01-01

Space-based assets, applications, user importance and maritime vulnerabilities

Lavers, CR

10.1117/12.2584920

Proceedings of SPIE - The International Society for Optical Engineering

Space-based assets, applications, user importance, and maritime vulnerability

Lavers, Chris, Moustakis, Fotios

Chris R. Lavers, Fotios Moustakis, "Space-based assets, applications, user importance, and maritime vulnerability," Proc. SPIE 11539, Technologies for Optical Countermeasures XVII; and High-Power Lasers: Technology and Systems, Platforms, Effects IV, 115390M (2 October 2020); doi: 10.1117/12.2584920

SPIE.

Event: SPIE Security + Defence, 2020, Online Only

SPACE-BASED ASSETS, APPLICATIONS, USER IMPORTANCE AND MARITIME VULNERABILITIES

Chris R. Lavers*[a], Fotios Moustakis*[a]

[a] Dartmouth Centre for SeaPower and Strategy, Plymouth University at Britannia Royal Naval College, College Way, Dartmouth, Devon, TQ6 0HJ; United Kingdom

ABSTRACT

Today we are reliant on a growing range of space-based assets. To assess inherent space-related risks it is critical to evaluate existing and planned systems. Here we summarise 2019-2020 findings from a wide range of participants. Our analysis includes: the importance of: persistency, all-weather, night and day capabilities, satellite image resolution, and other technical requirements. Hybrid threats, cyber warfare, GPS 'spoofing', jamming, and EMP are part of a new generation of threats becoming relevant with rapid space domain exploitation, in addition to space weather impact [**1**].
Keywords: Space-based platforms, applications, vulnerabilities

1. INTRODUCTION

Asset Infrastructure: A wide range of global systems, on: land, sea, air, and in space, are vulnerable to military or terrorist action, e.g. electromagnetic pulse (EMP), besides solar weather. These sources may affect more than just ECDIS and GPS. For unprepared space-systems operators, solar weather in its severest form can remove much of a ship's essential electrical infrastructure. Geomagnetic storms pose particular problems for space-based systems, such as GPS. When atmospheric transmission properties change unexpectedly, during storms, navigation fixes become inaccurate, and for short periods satellite signals may be lost completely. Protective measures against space weather are of vital importance to ESA, the EU, and the maritime community. Although GNSS has 3 critical segments: ground, space, and users, impact on space-based platforms directly impacts terrestrial users. Vessels are highly dependent on cyber-physical systems; navigation and control systems are vulnerable to solar weather and EMP. ECDIS, GNSS, and GPS system data provided by satellites for navigation and timing in turn feed ocean-going AIS, AIS compasses, GMDSS, besides other systems. Solar weather impact can be devastating, however deliberate targeting by EMP devices fitted to nanosatellites in the vicinity of critical space-based infrastructure could be as deadly, and if conducted in a coordinated manner, likely cause GPS and other networks to fail. Noise transmitted over GPS/GNSS frequencies raises levels to overload receiver circuitry, breaking signal lock; microwave or optical laser jamming can also deny, degrade or disrupt satellite performance.

1.1 Overview of Digital Maritime Surveillance Technology

Maritime surveillance today is cyber-space representation of what is happening over, on & under the physical domain of the sea surface and coastal areas, from various data products, to detect potential activities impacting security, safety, and economy of the environment. Space technology has supported maritime communities for over 30 years, benefiting them through enhanced navigation accuracy, GNSS (PNT) [**2**], and marine environmental monitoring and surveillance [**3**]. Sea poses unique challenges: small target detection; large survey areas; moving or changing targets and backgrounds. Maritime surveillance technology is a decisive factor in naval warfare and national security, and a force multiplier for successful operations. Advancing technologies play increasing roles in monitoring surveillance, relying on radar, and electro-optical solutions. Recently Synthetic Aperture Radar (SAR) and Inverse SAR (ISAR) have entered the operational theatre, providing opportunities in critical areas for Military or Civil authorities, with enhanced situational sea safety. Reduced space-based capabilities will significantly affect the ability to conduct maritime operations.

*christopher.lavers@plymouth.ac.uk +044 1803 677218; fax +044 1803 6772015;

Technologies for Optical Countermeasures XVII; and High-Power Lasers: Technology and Systems, Platforms, Effects IV, edited by David H. Titterton, Robert J. Grasso, Mark A. Richardson, Willy L. Bohn, Harro Ackermann, Proc. of SPIE Vol. 11539, 115390M · © 2020 SPIE · CCC code: 0277-786X/20/$21 · doi: 10.1117/12.2584920

Space-based capabilities Military requirements for detailed satellite imagery globally, 24/7/365, is driving satellite providers to reassess how they conduct business. The primary solution today is imaging radar, which operates under cover of darkness and in challenging battlefield or environmental conditions. The military market is significant, yet potential for civil exploitation is larger, with governmental and pan-governmental users (e.g. the EU's Copernicus programme) looking to provide detailed large-area views rapidly to end users. There are over 30 proposed satellite radar sensors, many of which will be realised. Key space-based capabilities include:

1.1.1 Synthetic Aperture Radar (SAR) Satellite-based SAR is used widely in maritime surveillance due to its ability of achieving high resolution in both range and azimuth directions [**4**]. Unlike optical imagery, SAR is unaffected by time of day, or meteorological conditions, meaning data acquisition can be made any time of day or night and independent of cloud coverage. When SAR satellite imagery is combined with Automatic Identification System (AIS) data in synergistic products, they provide a powerful tool for maritime surveillance, as AIS data can identify ships which SAR imagery detects, whilst SAR imagery detects ships which may not cooperate with AIS [**5**].

1.1.2 AIS AIS is an automatic tracking system used on ships and by Vessel Traffic Services, identifies and locate vessels by electronically exchanging data with nearby ships. It is used extensively in the maritime world with vessel AIS transponders using GPS receivers to collect vessel position and movement details. Maritime security and tracking are important AIS applications, with 250,000+ ships now broadcasting on AIS, allowing terrestrial detection up to 50km away. Due to earth curvature restrictions information is only available around coastal zones or on a ship-to-ship basis. One company Nano Satisfi is looking at LEO nanosatellite fleets to provide vessel positions without costly uplinks. Nanosatellites, typically 1-10kg in mass, are a recent maritime satellite solution, developed at low cost, and in numbers for threat resilience, but without the capabilities of traditional systems, previously only affordable by wealthy nations. These offer emerging countries and actors the ability to deploy spacecraft rapidly from development to launch. Nanosatellites can operate in co-operative ways, providing increased loss resistance, as well as being harder to target than existing maritime drones. Satellites solves this problem, whereby a ship's identity is recorded and decoded by satellite and sent to ground stations for further processing and distribution [**6**]. Known as S-AIS, it significantly increases the number of potential vessels within a satellite's footprint. Since the mid-2000s companies have detected AIS transmissions with satellite-based receivers. ExactEarth and Spire, alongside government programs, have deployed AIS receivers on satellites.

2. APPLICATIONS OF MARITIME SURVEILLANCE TECHNOLOGY

The potential applications of maritime surveillance technology include:

ISR- Intelligence, Surveillance and Reconnaissance encompasses multiple activities which relate to planning and operation of systems which support current and future military operations. Land, sea, air and space-based platforms have critical ISR roles in supporting operations.

Piracy- The worldwide threat of terrorism and piracy in international waters is high and the need for solutions is paramount. For piracy surveillance, and recent terrorist attacks on Saudi shipping (2018), satellite-based vessel detection can integrate with conventional data streams to extend surveillance information to Coastguard, police, naval, intelligence services, customs and border guards. Satellite imagery gives a unique overview of what happens around a hijacked ship, and can monitor movements of mother ships and smaller craft swarms. A Copernicus-funded project supported the Italian Coast Guard tracking the oil tanker *Caylyn Savina*, pirated in the Indian Ocean in 2011, using COSMO-Skymed constellation satellite imagery. Data collected is now effective in preventing attacks before they happen. Denial of satellite imaging will hamper such operations. It is likely satellite ship monitoring will tackle illegal immigration as imagery resolution improves.

Pollution and Oil Spill Surveillance- Oil slicks are visible in SAR imagery as dark areas. Most oil slicks are caused by ships emptying bilges before entering port. A satellite image can capture over 100,000km^2 of sea surface at once; an efficient way to check for oil spills. Satellite-based optical with SAR are of special relevance for oil spill detection, providing high-resolution all weather, day and night, wide-area coverage. CleanSeaNet, an European satellite-based oil

spill and vessel detection service, uses SAR images from polar orbiting satellites. CleanSeaNet identifies and traces oil pollution on the sea surface from ships and offshore installations, and monitors accidental oil pollution at sea during emergencies. Sentinel 1 is a satellite-based SAR system that supports operational oil spill monitoring and vessel detection and tracking in Europe [**7**]. Disrupted data reception may limit effective early response.

Ice Monitoring- Satellite-platform SAR data is valuable in monitoring seasonal or permanent ocean ice-cover in the Arctic, Baltic Sea, Bohai Sea, or Sea of Okhotsk. SAR images provide sea ice condition operational mapping for marine traffic or offshore operations. Sea ice cover change over recent years provides an indication of global warming, and is expected to strongly impact the Arctic environment. The Copernicus Marine Environment Monitoring Service (CMEMS) provides operational forecasts for sea ice to support Northern Sea ship routing, and search and rescue activities. The Sentinel-1A satellite allows frequent revisits (from daily). Satellite products are available (within 3 hours) to CMEMS operators who produce daily ice charts, iceberg density maps and maps of sea ice drift and deformation [**3**]. Infrequent data updates may increase collision risk.

Illegal Fishing- Illegal Unrecorded Unregulated (IUU) fishing has depleted fisheries to critical levels, yet IUU fishing persists as authorities cannot survey all seas simultaneously to stop it and protect marine species worldwide. London Economics (2015) reported 1 in 5 fish are taken illegally from the oceans, costing the global economy an estimated £15.2Bbn p.a. Fishing vessel behaviour monitoring is critical to tackle this problem. In the UK, a prototype Information Analysis Platform was developed to analyse fishing vessel behaviour, and can potentially use freely available satellite data from providers such as NovaSAR, Sentinel-1, or CubeSats, and data used by Defra, the Fisheries Departments and other authorities to inform of illegal fishing in UK waters [**8**]. Satellite imaging operates independently of AIS, but if satellite-based AIS and imaging reception are disrupted illegal fishing may go undetected.

Search and Rescue- Maritime surveillance technologies support search and rescue missions, detecting distressed vessels or missing aircraft or ships. Recent maritime operations have significantly changed priorities, providing a more effective approach to mass rescue operations highlighted by the Mediterranean crisis, and development of new search and rescue technology. Errors or outages in GPS information may hamper successful rescue of those in distress.

Illegal Trading of Goods- Maritime security threats include illicit activities, e.g. transport of migrants, smuggling goods, or drug trafficking. In the EU large amounts of cigarettes and tobacco are smuggled from China at an estimated cost to the EU economy of 10bn Euros *p.a.*, whilst drug smugglers use containerised sea transport as a simple, convenient and cost effective mode of transport as well as migrant transit [**9**]. NovaSAR is a constellation of 4 SAR satellites which once fully developed, will operate in all weather conditions, day and night. The UK allocated £21M to assist in development and launch of the first satellite in 2018. The Maritime Analysis and Operations Centre –Narcotics (MAOC-N), based in Lisbon, is an EU initiative involving 7 countries. The Centre uses integrated vessel information to monitor and track suspect vessels in the Atlantic and Mediterranean [**10**].

Other threats, satellite imaging and RF detection may assist include:

Anti-Terrorism Activities- Ships and seaports may be used to facilitate terrorist activities in different ways including: using ships as 'bombs'; and weapons trafficking. Operation Active Endeavour (OAE) is a maritime surveillance operation led by NATO's naval forces which patrol the Mediterranean and monitor shipping to help detect, defer and protect against terrorist activity. The operation evolved following terror attacks against the USA (Sept. 2001.)

Port and Off-Shore Security- refers to the defence, law and treaty enforcement, and counterterrorism activities that fall within the port and maritime domain, including protecting seaports and harbours by monitoring facilities, storage areas and container depots. Current systems operate by scanning and observing all land and maritime zones for unauthorised activities continuously. If intruders are observed, the systems continue with identification and tracking of the intruders and direction of security forces.

Autonomous Boat Navigation- Rolls-Royce began developing unmanned technology in 2013 and expects by 2025 there will be satellite remote controlled unmanned coastal vessels, and ocean-going ships by 2035. GPS reception disruption and consequent AIS output for unmanned vessels, will have a significant impact.

Land-based Applications- Surveillance can gather information to support maritime-based activities, and provide benefits in observing and supporting land-based activities in the littoral environment. Applications include: Agriculture: Forestry:

Risk Management, and Disaster Monitoring: where satellites monitor areas affected by disasters e.g. flooding, tsunami, critical for timely disaster relief efforts, allowing for rapid response to priority areas captured in images.

3. SPACE PLATFORM THREATS

Good cyber-security at organisational and personal levels is essential if threats to space-based GPS, AIS, and other data are to be neutralised effectively. The size of geospatial vectors in raster and point cloud data make them obvious targets for computer-based-learning algorithms. The importance placed on GPS, and AIS by end users is clear. Subversive space-based attacks on GPS-satellite platforms will likely attempt exploitation by new methods as well as traditional attacks. Likely attack routes include: jamming, EMP devices, direct satellite destruction (bomb or kinetic device), or laser-based weapons. Anti-satellite (ASAT) demonstrations prove kinetic capabilities; a recent Indian ASAT test took place at an altitude low enough that debris burned up in the atmosphere [**11-12**]. Kinetic systems create permanent and irreversible space asset destruction, whilst electronic and cyber provide temporary disruption and damage to space systems. Some states are moving away from expensive consumable direct-ascent missiles to affordable and available long lasting electronic and cyber methods that impact space assets. In addition co-orbital satellite systems (COSAT) systems are satellites place on similar orbits directed to intercept or interfere with other adjacent satellites through close orbital rendezvous operations. Threats may also be provided from high altitude pseudo-satellite platforms.

GPS jamming or spoofing of a satellite may prevent ephemeris ground station updates. A small space jammer can disrupt the satellites GPS signal reception as effectively as a small terrestrial GPS jammer can disrupt proximity receivers. Protocol-specific attacks [RF] or 'messing with in-built commands.' attack systems through flaws in data protocols, and Software-specific attacks [SW] or 'messing with the data'. Implementation threats exploit vulnerabilities in service provider systems, attacking collection and vessel information visualisation. Ground station update authentication must ensure transmitters are genuine, and time-stamped. Integrity tampering is vital so valid data checks are required, e.g. is geographical information correct and of the expected type? Data location must be cross-checked across other valid data sources. Fake reports or numerous false GMDSS satellite alarms may be broadcast, triggering satellite response. Spoofing 'hijacks' a satellite's command and control, and feeding it false data is a known means of disruption, available to the US since 2004. We must build protection for critical space-based infrastructure, covering space, maritime and terrestrial systems, for military and civil operations. At present the main protection means from solar weather is increased warning time. However, co-ordinated attacks from nanosatellite threats may happen without warning. Satellite swarms may provide some protection against sudden catastrophic system loss, but 'hunter-killer' nanosatellites armed with EMP generators may degrade systems overall. Hardening all space-based systems to military grade EMP protection is unfeasible, nor affordable. Early examples of Chinese scientists 'blinding' optical satellites with ground-based laser guns (2005), were followed by Russian Federation laser-based A-60 aircraft ASAT operation, dazzling and blinding sensors to result in physical damage. In each case correct threat hazard evaluation from multiple intelligence sources and integration will determine various courses of action, likely objectives, desired outcomes, and how to prioritise them.

4. STAKEHOLDER QUESTIONNAIRE RESEARCH METHOD

Surveillance technical capabilities-: From 4 years of discussion with civilian and military global space and maritime professionals we report their views on current and future space-based requirements, coming from upstream satellite data providers and launchers, as well as the downstream user sector. Consultation took place via face-to-face interview, telephone consultation, email or questionnaire. We received responses from 90 stakeholders and we summarise this engagement from these responses. Respondents indicated specific capabilities of space surveillance systems importance, rating importance of 'night & day', 24/7 capabilities; 'all-weather' capability, and 'persistency', on a scale of 1 (not at all important) to 5 (very important) and were asked about AIS, data-acquisition temporal frequency requirements. Maritime professionals stated the most important capability with geographical interest. Analysis, taken with other data revealed the types of service/s of interest to participating organisations with weighted importance, differing by nation and between upstream or downstream. Fig.1 provides the geographical distribution of the questionnaire respondents, with breakdown by global region. Ninety stakeholders gave answers to some or all of the questions presented.

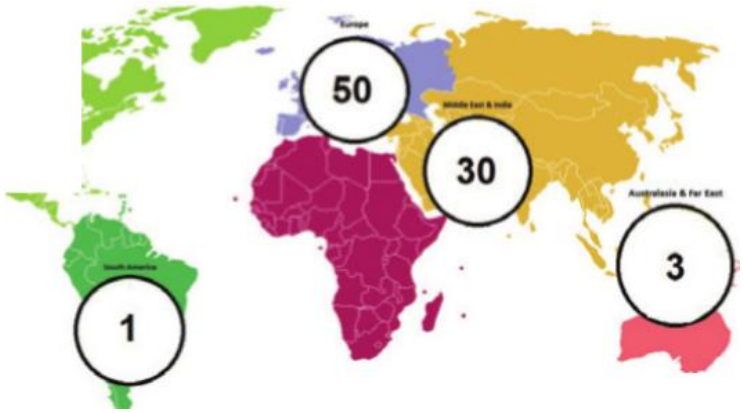


Figure 1. Distribution of Stakeholders' views.

5. RESULTS AND DISCUSSION

Persistency: providing maritime/littoral surveillance of an area for prolonged periods is a high requirement for downstream satellite users. Ten Middle East Downstream responses, from 3 nations, had very high regard: 90% responding 4-5 (Fig. 2). Typical comments: "*The persistent system would be required in the event of a piracy incident, enabling surveillance of movement of hostages*"; a common criticism was "*We do not have the capacity to process data any faster than weekly, except in crisis conditions following a piracy incident*." Eleven Upstream Company returns (Fig. 3) from launch sector companies gave good correlation with downstream categories (4-5). It may be inferred upstream companies are judging the end-user market well.

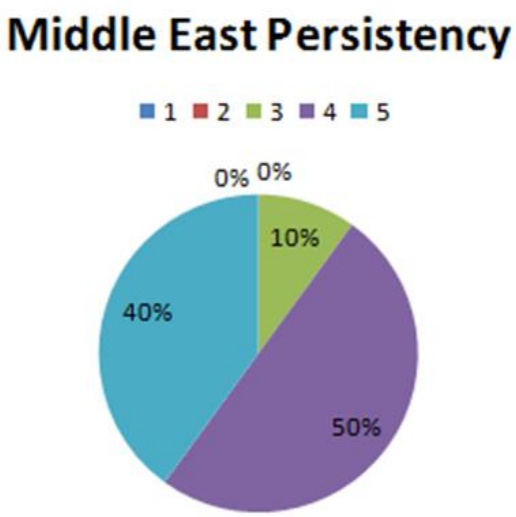


Figure 2. Middle East Downstream Persistency Responses.

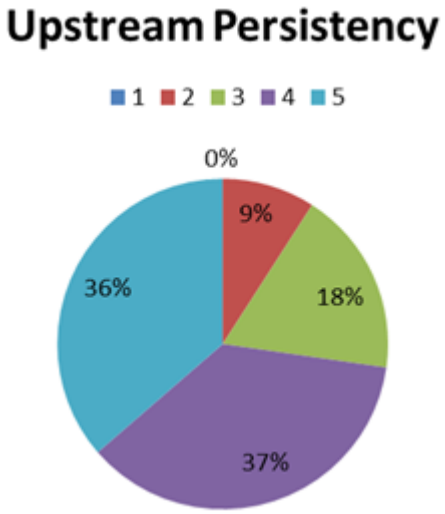


Figure 3. Downstream Persistency Responses.

Combining together both the upstream and downstream response from the 31 individual sources a more balanced overall assessment is provided (fig 4.)

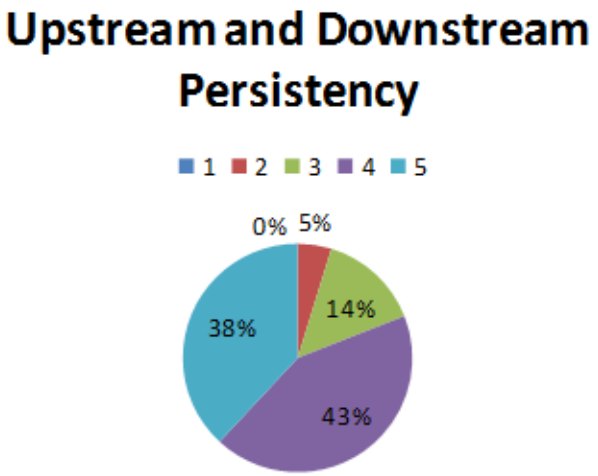


Figure 4. Persistency Upstream and Downstream results.

Night-Day capability Qatari Coastguard End user 'Night-Day' importance data is shown (Fig. 5). Typical responses: "*Because you want a safe coast you have to work night and day and in all weather conditions*," and "*Our mission has to be done 24/7 partial coverage would not offer the operational capability requirement*."

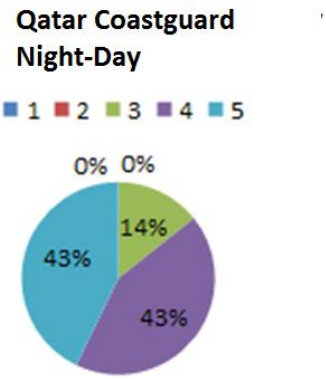


Figure 5. Qatar Coastguard Night-Day.

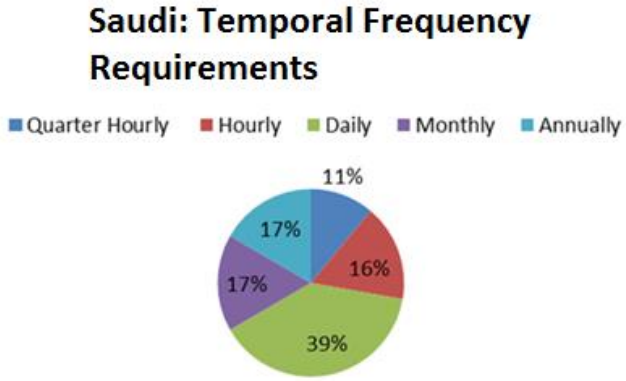


Figure 6. Saudi Arabian Temporal Frequency Requirements.

Temporal Surveillance The perception of temporal range requirements from thirteen Saudi Arabian end-users, are spaced a cross the range (Fig. 6), but favour at least daily measurements. Frequency requirements vary. Some respondents gave more than one answer. One South American response on this temporal issue stated *"An hourly frequency is enough to hail all ships inside the area of maritime operation."* Another UK response "*Guaranteed daily, and then hourly when needed would be very useful for flooding applications."* There is no universal specific frequency requirement but frequency requirements are universal.

Current resolution requirements are extremely variable. For general updates of the maritime picture daily updates are sufficient, i.e. domain (fig 7.) In terms of target selection type, (fig. 8), skiffs up to 10m and small fast boats c. 20ft provide a dominant category 43%. 1-3m resolution allows vessel recognition, whilst 300m+ is sufficient for tankers or large ships. 10% state sub-km resolution, nearly ¼ require 1-30m medium resolution. 16% want optical resolution below one metre, and 25% of respondents state they require high resolution SAR. Nearly ¼ of end-users require domain awareness. Responses from 14 upstream/downstream stakeholders show Fast boats/skiffs are the main category, which if combined with 5m accounts for 72%. One Qatar response "*4-5m rib, look for clear view of any vessel entering Qatar Coast illegally to be able to complete successful mission without putting any Coastguard personnel in danger*."

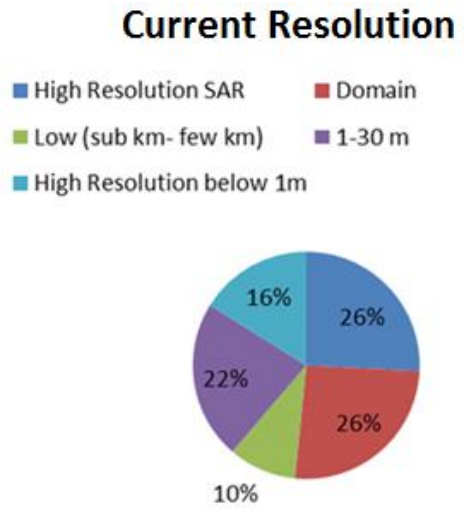


Figure 7. Current Resolution.

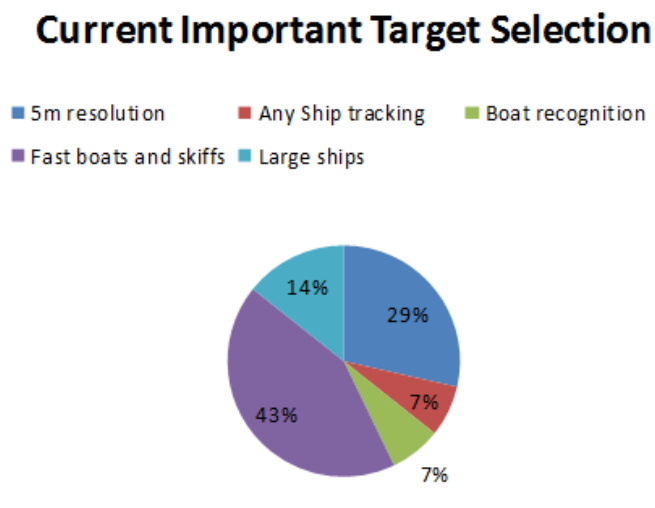


Figure 8. Target Selection.

Most important space-based capability we gauged perception of the importance of sensing and communications abilities from various maritime professionals. 33 UK respondents provided evidence of the overwhelming importance of GPS, being the single-most important space-based capability (Fig. 9).

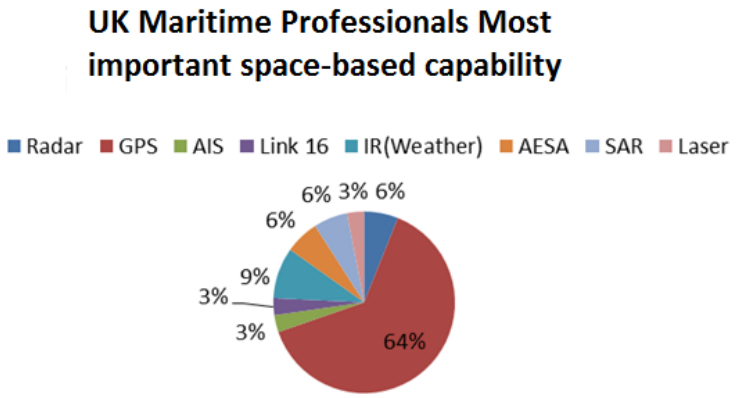
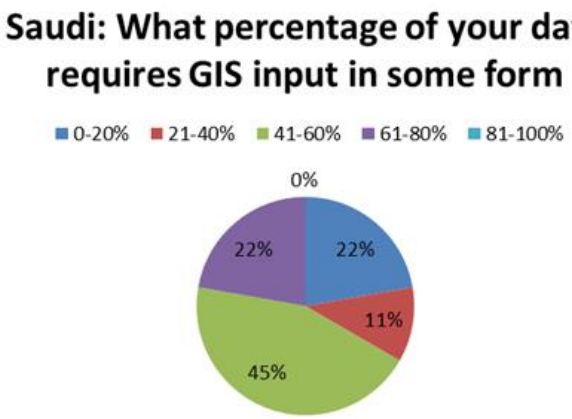


Figure 9. Most important capability.

The importance of GIS, usually reliant upon GPS input, is clear in fig. 10 from the Saudi Arabian response to "*what percentage of your data requires GIS input in some form*"? Clearly the biggest category with nearly half of respondents (18) required 41-60% of data of a geographical information system-related nature, e.g. AIS. This view is further confirmed by Qatar respondents on the importance of AIS capabilities fig. 11.



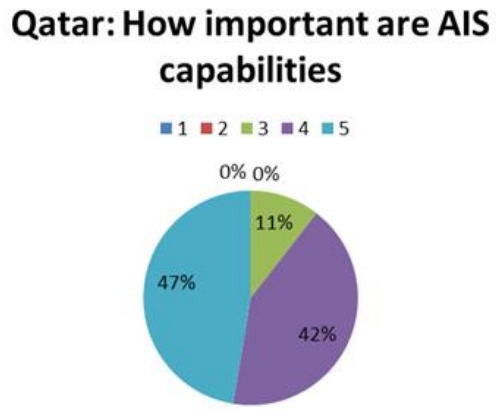


Figure 10 Importance of GIS to Saudia Arabian responses. Figure 11 Importance of GIS to Qatar responses.

All-Weather capability: Nine Downstream Qatar respondents indicated here, this capability was dominant, i.e. very important, with eight out of nine responses in categories 4-5 (fig. 12). A typical Coastguard response of all-weather capability is clear, "*It will manage the coastal area and offshore area in bad weather when small boats cannot go offshore."*

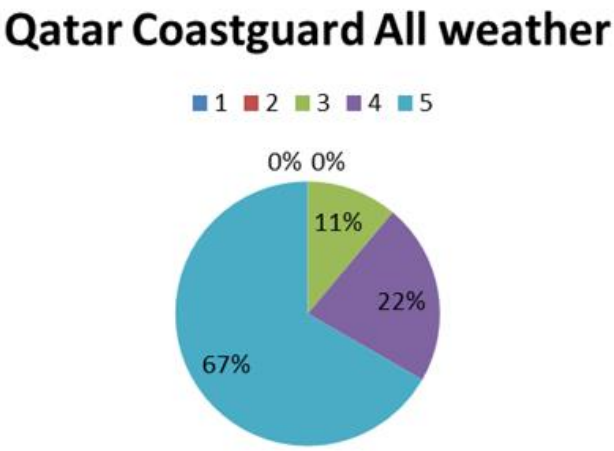
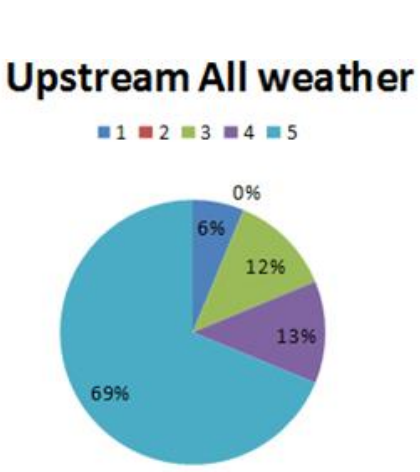


Figure 12. All-Weather Capability

The Qatar downstream All weather requirements correlates very well with the overall upstream results from sixteen corporate correspondents (fig 13.), and also with the combination of all upstream and downstream responses (fig 14.)



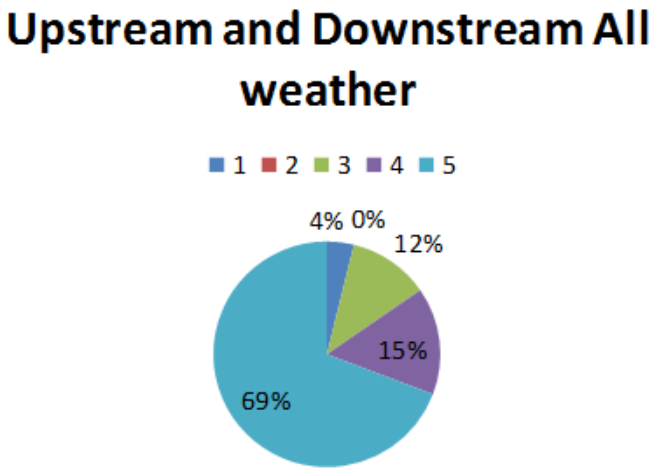


Figure 13. Upstream All-Weather Capability. Figure 14. Upstream and Downstream respondents (26 responses).

6. SUIMMARY

This paper provided discussion of current space-based assets, applications, importance and vulnerabilities, with quantified findings covering: persistence, Night-Day, S-AIS, surveillance frequency, resolution and target selection, with all-weather capabilities. Some market-players interviewed stress the trend towards Smart Data Analytics, with mixed optical/SAR tailored information, improving SAR utility and earth observation data. SAR is a strong market-area within maritime persistent stare, supporting commercialisation of space-based high resolution SAR with other capabilities, likely in consortia composed of multiple partners. One UAE respondent expressed the aspiration for "*A satellite which can provide earth imaging, detecting piracy, reckoning and illegal ships*". Expectations, in some cases between upstream and downstream are well-matched, and less so in other categories. Mismatch between user and supply groups is important, and shows there is work to be done gauging and bridging demand for specific customer services, matching upstream with downstream users. The range of responses is considered representative of the space-based maritime security and surveillance markets, which have grown in recent years and will continue to grow over coming decades. With increased use of advanced on-board processing, all digital components, software-defined radios, packet-based protocols, and high performance cloud-computing, the attack potential for cyber and physical attack is greatly expanded.

7. REFERENCES

[1] Lavers, C.R., Moustakis, F., Space-Based assets, Applications, user importance and Cyber Vulnerability in Maritime Operations, NATO Maritime Interdiction Operational Training Centre, pp 6-12, Issue 20, 1st Issue 2020, ISSN: 2242-441X (2020).

[2] UK Royal Academy of Engineering Report: "Global Navigation Space Systems," <https://www.raeng.org.uk/publications/reports/global-navigation-space-systems> (22 September 2020).

[3] ESA <https://www.esa.int/Applications/Observing_the_Earth/Copernicus/Why_is_space_relevant_for_maritime_issues> 22 September 2020)

[4] Guerriero, M., Willett, P., Coraluppi, S., and Carthel, C. Radar/AIS data fusion and SAR tasking for maritime surveillance. In Proceedings of 11th international conference on information fusion, (2008).

[5] “Satellite Imagery helps to monitor the seven seas” <https://geocento.com/satellite-imagery-case-studies/satellite-imagery-can-help-on-maritime-surveillance/> (22nd September 2020).
[6] <https://www.esa.int/Applications/Telecommunications_Integrated_Applications/Satellites_for_safer_seas esa.int/Our_Activities/Telecommunications_Integrated_Applications/Satellite_-_Automatic_Identification_System_SAT-AIS> (22 September 2020).
[7] “Maritime Monitoring” <https://sentinel.esa.int/web/sentinel/user-guides/sentinel-1-sar/applications/maritime-monitoring> (22 September 2020).
[8] <https://www.waittfoundation.org/practioner-resources> (22 September 2020).
[9] “Migration to Europe”<economist.com/blogs/graphicdetail/2015/09/migration-europe-0> (22 September 2020).
[10] “Sea Border Surveillance”, <cordis.europa.eu/result/rcn/90108_en.html> (22 September 2020).
[11] Rajagopalan, R.P. “India’s Changing Policy on Space Militarization: The Impact of China’s ASAT Test”, India Review Vol. 10, No.2, pp. 354-378, (2011).
[12] Rajagopalan, R.P., “Having Tested its ASAT Capability, India Should Help Shape Global Space Norms”, ORF Commentaries, March (2019).